STANDARD FORM NO. 64 ~~CONFIDENTIAL~~

Office Memorandum • UNITED STATES GOVERNMENT

TO : Mr. Walter Pforzheimer

DATE: 7 March 1947

260

FROM : Chief, Communications Division

SUBJECT: CIG Enabling Act

1. I believe that the act as written can be interpreted to include foreign intelligence derived from cryptanalytic effort. However, it would probably be better if it were spelled out to give CIG this specific authority. This could be accomplished by merely adding words so that the proper portion of the act would read "Foreign intelligence including that derived from cryptanalytic effort, etc."

2. There are many arguments in favor of centralizing cryptanalytic work. A few non-technical reasons are the following.

a. Centralized effort is more economical since it avoids all duplication and overlap.

b. It makes the best cryptnalytic personnel in the country available at one place to attack all problems regardless of responsibilities.

c. It accomplishes centralization of an extremely valuable source of intelligence in CIG, thereby greatly furthering the basic purpose of establishing CIG.

d. It is a major step in overall coordination of U.S. foreign intelligence.

e. It will enable the various sections of CIG to work with greater effect by pooling intelligence requirements and targets.

f. The centralizing of cryptanalytic work and combining it with all other intelligence sources will do more to prevent another Pearl Harbor than any other single thing that the U.S. Government can accomplish by permitting all foreign intelligence to meet at a common point where an accurate evaluation of the meaning of the intelligence can be drawn and a quick dissemination made to responsible Government agencies.

3. There are a number of technical reasons favoring centralized cryptanalytic work. Without going into too much detail or being too specific, a few of these are roughly as follows: (Note, however, that specific exceptions can be made to nearly every statement that follows.)

~~CONFIDENTIAL~~

a. Problems are common between different users, since there are only a limited number of satisfactory cryptographic means at their disposal. It is nearly impossible to draw a sharp dividing line between user A and B. Assume that both use the same basic system, the problem then, generally, is the same basic problem and requires personnel with the same qualifications and training to solve. Why establish two separate camps with two sets of duplicate effort to do the same work? Liaison is far from an ideal solution.

b. If work is divided between two agencies as it must be, on what basis will the division be?

(1) A message is intercepted, division is on basis of contents of message, i.e. clandestine, Army, Navy, Air, Foreign, etc. One key used may and often does contain messages for all agencies, in which case it is impossible to determine who should work on the message until after it has actually been deciphered! Who is in a better position to work on this message than a central group with even responsibility to all U.S. agencies?

(2) Division is on a basis of types of cipher. One of the most difficult parts of cryptanalysis is determination of how the message is enciphered. Hence, in studying a new system who does the work? Usually solution is well under way by the time the type is determined - so then you find it is not your type after all and it is transferred to the other agency. The background you have built up is lost and you start over on something else instead of continuing to the end result or calling in the specialists to contribute to your background.

4. Centralization does bring up a number of problems. A recommended solution is briefly as follows:

a. Centralization of all cryptanalytic effort.

(1) Officers from Army, Air Force, Navy, State, etc. to be detailed to take care of primary requirements of the various services.

(2) Field stations were required to be provided by the central group with that group retaining general direction and supervision of the stations. Personnel to be for the most part from the service requiring the station. Close coordination kept with CIG.

b. Intercept responsibilities to be controlled by CIG, but each service to maintain primary responsibility for interception and D.F. (when required) of its specific targets. (i.e. Navy primarily responsible for Navy interception and D.F., etc.)

(1) Commercial and clandestine intercept the primary responsibility of CIG.

(2) System must maintain flexibility and cooperation to achieve overall maximum results with some sharing of facilities.

5. Connected with this overall problem are two others which should be considered, both bearing on security.

a. Cryptographic security of U.S. agencies should become a function of CIG. This is essential to afford agencies the advice and experience of the cryptographic personnel of CIG, the one point where the best qualified personnel in the U.S. are concentrated. This is further essential to avoid errors and poor judgment by non-qualified personnel.

(1) Should extend to making CIG responsible for development, production, etc. of all U.S. cryptographic means, etc.

(2) However, the prerogative of commands, etc. cannot be ignored. Hence, in special cases CIG action should take the line of advising dangers, limitations, etc. with proper recommendations to commands. But final decision rests with the commander. Exception - transmittal of CIG intelligence by other agencies will be restricted to specific cipher and means authorized by CIG. Also, CIG can prohibit the transmission of Secret and Top Secret material over certain ciphers.

b. As a desirable feature to insure maximum security of intelligence and sources, although not essential, would be the establishment of a network of CIG personnel for the purpose of handling intelligence material, acting as liaison officer, and CIG channels to and from U.S. field agencies to serve the double purpose of forwarding material to CIG and disseminating CIG high level intelligence to field agencies. For example - CIG liaison officer would be established with major U.S. Army or combined headquarters and like offices. His function is that of CIG advisor to the commander and channel for the flow of CIG intelligence reports. He would maintain his own cipher facilities, which may extend to operating his own communications facilities.

25X1

Colonel, GSC
Chief, Communications Division

CONFIDENTIAL